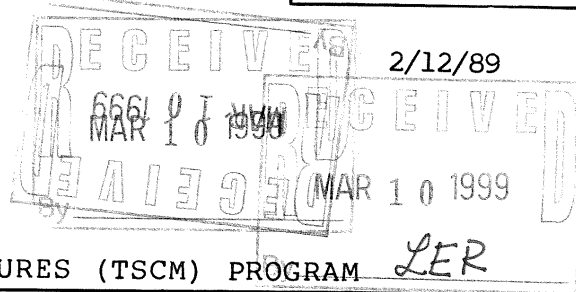


ORDER

U.S. DEPARTMENT OF TRANSPORTATION
FEDERAL AVIATION ADMINISTRATION

1600.12C

**AUA TAC
DOCUMENT MANAGEMENT
CENTER**



SUBJ: TECHNICAL SURVEILLANCE COUNTERMEASURES (TSCM) PROGRAM LER

1. PURPOSE. This order provides for a Technical Surveillance Countermeasures Program in accordance with Order DOT 1600.16B, Technical Security Countermeasures Program, dated June 4, 1981. It is designed to establish procedures, standards, criteria, operational and classification guidance for TSCM surveys/inspections, which are functions of the Office of Civil Aviation Security (ACS). Appendix 1 provides information and guidance concerning physical security in sensitive areas required to support TSCM operations.

2. DISTRIBUTION. This order is distributed to the division level and above in the Washington headquarters, regions and centers, and overseas area offices. Limited distribution is made to all field offices and facilities.

3. CANCELLATION. Order 1600.12B, Technical Security Countermeasures Program (U), dated February 4, 1974, is cancelled.

4. BACKGROUND. Executive Order 12356, National Security Information, established governmentwide requirements for measures to protect national security information from unauthorized disclosure in any form. This includes compromise through technical surveillance, e.g., through the use of "bugs" and other surveillance techniques.

5. DEFINITIONS.

a. Technical surveillance countermeasures are techniques and measures to detect and neutralize a wide variety of hostile penetration technologies which are designed to obtain unauthorized access to classified and sensitive information. Technical penetrations include the employment of optical, electro-optical, electromagnetic, fluidic, and acoustic means as the sensor and/or transmission medium, as well as modification to equipment or building components for the direct or indirect transmission of information meant to be protected. TSCM methodologies include detection and neutralization of hostile penetration efforts against telephones and telephone systems, equipment, conference rooms and office areas used for the storage, discussion, and handling of classified information.

b. TSCM survey is a complete electronic and physical examination of an area for the purpose of identifying technical surveillance devices or systems.

2/12/89

after completion of the survey. Upon arrival, the TSCM team will contact the POC and conduct the survey/inspection. When the survey/inspection has been completed, the TSCM team will give an exit briefing covering the findings of the survey/inspection. A formal written report will be provided subsequently.

10. FUNDING. ACS-300 will fund all surveys except for one-time conferences or meetings and special requests for TSCM support which are to be funded by the requester.

11. DISCOVERY PROCEDURES. Upon discovery of a suspected eavesdropping device, the following actions will be taken:

a. The area will be secured to prevent attempts by the eavesdropper to remove the device. In a nonalerting manner, action will be taken to cease the discussion or processing of classified information in the area while, at the same time, preserving, to the extent possible, the normal work atmosphere. No attempts will be made to remove the device at this time.

b. A report will be submitted without delay to ACS-300 via "IMMEDIATE" message, classified SECRET (use another agency's communications system if the communications center is involved). As a minimum, the message will contain the following:

- (1) Time and date of discovery
- (2) Area or facility involved
- (3) Specific location of the "find"
- (4) Method of discovery
- (5) An estimate as to whether the eavesdropper was alerted to the discovery
- (6) Describe the known or suspected compromise involving the cryptocenter operation

c. Notify the senior responsible official of the discovery and of the actions taken.

d. Information concerning the "find" will not be released to other persons or agencies not directly involved until such release has been coordinated with, and approved by, ACS-300.

e. No effort will be made to test or to attempt to remove the device until ACS-300's reply to the preliminary report is received authorizing such actions.

f. ACS-300 will advise the Office of Security, M-70, and others, as required. If cryptographic communications of facilities are involved, reports to the National Security Agency and the U.S.

Air Force Cryptologic Support Center will be made. In facilities having SCI, the Central Intelligence Agency will also receive a report.

12. CLASSIFICATION GUIDANCE. In addition to the OPSEC requirements outlined in paragraph 7, the following classification guidance will be adhered to in accordance with NSCG, HHB 70-9, dated August 1, 1982:

a. All information concerning timing, location, equipment, or methodology employed in a TSCM survey (or its results) which, if divulged, would tend to aid in circumventing the survey is classified SECRET. This includes all correspondence and discussion regarding requests for pending TSCM surveys and results of completed surveys/inspections.

b. Information concerning physical security devices and techniques which, if divulged, could aid in the physical or electronic penetration of intelligence facilities is classified SECRET.

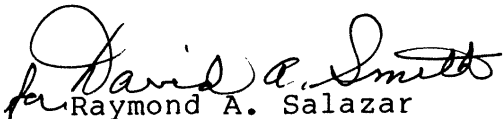
c. Information concerning the design, construction, and internal communications systems of intelligence facilities which, if divulged, could aid in their penetration is classified SECRET.

d. Information concerning the discovery of a suspected technical surveillance device is classified a minimum of SECRET, with additional special handling instructions, as appropriate.

13. CLASSIFICATION MARKINGS. All classified TSCM correspondence shall be marked in accordance with requirements of Order 1600.2C, to include the following caveat and regrading data:

"WARNING NOTICE:
INTELLIGENCE SOURCES OR METHODS
INVOLVED (WNINTEL)"

"Classified by: (Enter name and code)
Based on: NSCG, HHB 70-9, of 8/1/82
Declassify on: OADR"


Raymond A. Salazar

Director of Civil Aviation Security

Attachment

2/12/89

APPENDIX 1

PHYSICAL SECURITY GUIDANCE

1. Physical security is the most important countermeasure to technical penetration. Access to a facility or space or, at a minimum, to its immediate vicinity, must be gained before a penetration can be accomplished. To understand the importance of the requirements for good access controls, an appreciation of the various technical penetration capabilities must be gained.

a. Wired Microphones. A technical surveillance penetration employing a wired microphone against an area with good physical security is difficult to accomplish. The task is made much simpler if the area contains unused wiring. By using existing wire runs which exit the secure perimeter, a technical penetration can be accomplished in a minimum amount of time without introducing potentially alerting additional wire.

b. Telephones and Intercommunications Systems. Modified telephone and intercommunications systems can provide a highly exploitable means of retrieving audio from a space without installing wiring. This type of penetration is a universal threat because spaces in which sensitive classified discussions occur often contain at least one telephone or intercommunications unit. No telephones should be installed in secure discussion areas unless absolutely mission essential and then only when prior approval has been obtained from ACS-300.

c. Radio Frequency (RF) Transmitters. Recent technical penetration discoveries reveal a continued trend on the part of hostile intelligence services to employ RF transmitters. This is due largely to advances in technology which allow extremely small and efficient transmitters to be designed for quick installation. They are disguised often as part of an ordinary piece of office furniture. Discovery of RF transmitters is complicated further by their use of complex modulation schemes and remote deactivation capabilities which reduce the time they are detectable and conserve battery power.

d. Tape Recorders. Miniature tape recorders which permit several hours of recording have been improved greatly and must be considered more of a technical penetration threat than was true in the past. Should unescorted visitors, who are not cleared properly, have routine access to sensitive areas, such devices can be installed quickly and removed later or serviced with only minimal risk of detection.

e. Optical Devices. Protection from long-range optical penetrations must also be considered. Visual and optical

surveillance of areas where classified material is discussed and maintained is a viable method of technically penetrating a secure area.

2. For the most part, providing physical security measures to protect property and material will be useful in preventing technical penetrations. Additional precautions must be applied to those areas in which classified discussions are routinely held. While adequately preventing surreptitious entry into a room, conventional measures may do nothing to preclude retrieval of audio via an unprotected conduit, such as an uncovered window or an air conditioning duct. Physical security protection must extend also to areas surrounding the space needing protection. By providing a buffer area around a secure space, many audio security vulnerabilities can be avoided.

a. Audio Paths. All openings and electrical conduits which may pass intelligible audio to an uncontrolled area must be sealed. Ducts can be baffled acoustically to control audio which could otherwise be retrieved.

b. Excess Wiring. All conductors, including those servicing telephone, intercommunications, and electrical systems, as well as other types of fortuitous conductors, should be identified to ensure that they are required. All extraneous and unused conductors should be removed or shorted together and grounded within the secure area to preclude their use as part of a clandestine surveillance system. Exploitation of such wiring would facilitate audio penetration attempts.

c. Escorts. All individuals allowed into sensitive areas should be appropriately cleared or escorted. Introduction of audio devices into a space can be effected quickly, even by relatively untrained personnel. Routine access by uncleared personnel and building maintenance workers can provide ample opportunity for implanting a relatively undetectable eavesdropping device. The risk is of particular concern in overseas locations where indigenous personnel may be used for this purpose. All uncleared personnel entering controlled access areas must be closely escorted by cleared personnel who have been briefed thoroughly on the technical penetration threat. Escorts should not only be alert to their charges removing items but also to the possibility that a device could be left behind. Cleared personnel should be used for housekeeping services in highly sensitive locations whenever possible, especially overseas. A log of all repairs and alterations to the space should be kept to include the identities of the individual workers and the types of repairs accomplished. This will provide a history of events occurring within an area and aid in identifying perpetrators of any possible clandestine installation found later.

2/12/89

3. Sound Masking. Secure areas cannot always be isolated from adjoining spaces to preclude either inadvertent or deliberate eavesdropping. Where space configurations and usage bring about this circumstance, classified conversations may, under controlled conditions, be masked by an artificially introduced noise source. This can be accomplished by installing a specially designed tape system (not radio) within the secure area and directing the sound from special prerecorded tapes at a specified volume at those areas where eavesdropping devices might be planted. Speakers used as components of such a system can be installed in plenums and ducts. To provide the intended protection, the artificial noise must be at a much higher decibel level than the sensitive conversation. Methods of attaining this objective include coupling the noise source to the walls, floor, ducts, windows, pipes, etc., using transducers. Another approach is to provide a barrier such as a false wall, heavy floor-to-ceiling draperies, or a false ceiling between the speakers and the critical discussion areas. The noise is injected into these spaces to lessen its interference with the conversations taking place. Any sound masking system must be approved by ACS-300 before installation.

4. Equipment/Furnishings. All furnishings and equipment should be mission essential, and should be dedicated to the secure area. Because furnishings and equipment can be used to introduce concealed surveillance devices into an area, special precautions are required. Each item should be inspected physically by a person familiar with the furniture or equipment prior to its being placed in the secure area to detect any anomalies or suspicious features. Equipment/furnishings introduced into the controlled space must be checked by qualified TSCM personnel during the next scheduled TSCM support service to the area. Equipment which processes classified information often represents a technical security risk by emanating radio frequency signals into free space and onto existing wiring (power, telephone, intercommunications, etc.) serving a facility. Inspection requirements and specific countermeasures for this equipment fall under the purview of the TEMPEST program which is defined in other directives. The use of nonmission essential radios, recorders, televisions, and other electronic devices in areas designated for the discussion of classified information is prohibited.